
Veštačka inteligencija između inovacija i regulacije

Apstrakt

Ubrzani razvoj sistema veštačke inteligencije (VI) iznova postavlja pitanje ravnoteže između podsticanja inovacija i zaštite javnih interesa. Ovaj rad analizira aktuelne međunarodne regulatorne okvire – pre svega Evropski zakon o veštačkoj inteligenciji (AI Act, 2024), Opštu uredbu o zaštiti podataka (GDPR) i ključne standarde ISO/IEC serije – i sagledava njihove implikacije za regulatorni razvoj u Republici Srbiji. Posebna pažnja posvećena je procesu izrade prvog Zakona o VI u Srbiji, strateškim dokumentima koji usmeravaju razvoj digitalne ekonomije i obavezama koje proističu iz procesa pristupanja Evropskoj uniji. Rad argumentuje da sveobuhvatan, na riziku zasnovan pristup regulisanju VI ne mora biti prepreka inovacijama, već može postati osnov za izgradnju poverenja korisnika, pravnu sigurnost privrednih subjekata i dugoročnu tehnološku suverenost.

Ključne reči: veštačka inteligencija, regulacija, AI Act, GDPR, ISO/IEC 42001, Srbija, digitalna transformacija, upravljanje rizicima, pravni okvir, standardi, inovacije

Uvod

Veštačka inteligencija postala je jedna od najznačajnijih tehnoloških paradigmi 21. veka. Sistemi zasnovani na mašinskom učenju, obradi prirodnog jezika i računarskom vidu nalaze primenu u zdravstvenim dijagnostičkim sistemima, autonomnim vozilima, finansijskim instrumentima za predikciju rizika, sistemima sudskih preporuka i javnoj upravi (Russell & Norvig, 2021). Upravo zbog ove duboke integracije u kritične društvene procese, VI postaje interesantna zakonodavcima koji nastoje da regulišu upotrebu, ali ne i razvoj (Calo, 2017). Ubrzani razvoj sistema zasnovanih na mašinskom učenju i velikim jezičkim modelima donosi izuzetne mogućnosti za automatizaciju procesa, unapređenje produktivnosti i stvaranje novih vrednosti, ali istovremeno otvara složena pitanja koja spadaju ne samo u domen tehničko-tehnološkog

razvoja već i etike, zaštite ličnih podataka, ljudskih prava, autorskih prava, bezbednosti i drugog. Ovaj dualizam između inovativnog potencijala i rizika čini regulaciju veštačke inteligencije jednim od najizazovnijih normativnih zadataka savremenih pravnih stručnjaka.

Postojeći pravni okviri pokazuju ozbiljne nedostatke i nedostatak fleksibilnost da adekvatno regulišu rizike koji nastaju primenom VI. Dosta faktora utiče na kompleksnost pravnog uređivanja primene VI, a tu spadaju: nepredvidivost ishoda, ko snosi odgovornost, pristranost uzrokovana podacima za treniranje VI, kao i nepredvidivost i istinitost sistema i modela u realnim okruženjima (Doshi-Velez et al., 2017). Ovaj regulatorni jaz motiviše novu generaciju zakonskih inicijativa, od kojih je Evropski *AI Act* (2024), za sada najpotpuniji.

Na globalnom nivou, različiti akteri pristupaju regulisanju veštačke inteligencije sa različitim filozofijama i prioritetima. Evropska unija je u martu 2024. godine usvojila Akt o veštačkoj inteligenciji, koji predstavlja prvi sveobuhvatni propis o veštačkoj inteligenciji na svetu, zasnovan na pristupu zasnovanom na riziku (*risk-based approach*). Sjedinjene Američke Države su se opredelile za fleksibilniji, tržišno orijentisan pristup, uz značajno smanjenje regulatornih ograničenja. Ujedinjene nacije su u martu 2024. godine usvojile globalnu rezoluciju o sigurnoj, bezbednoj i pouzdanoj veštačkoj inteligenciji za održivi razvoj. Ovaj regulatorni mozaik odražava duboka razmimoilaženja u pogledu ravnoteže između razvoja i inovacija sa jedne strane i zaštite javnog interesa i korisnika sa druge strane.

Cilj ovog rada jeste da predstavi ključne elemente međunarodnog regulatornog i etičkog okvira i sagleda mogućnosti i pravce regulisanja VI i perspektive razvoja zakonodavnog okvira u Republici Srbiji. Metodološki pristup kombinuje normativnu analizu pravnih tekstova, komparativnu analizu regulatornih strategija i pregled naučne literature.

Pravni i etički okvir

Međunarodni regulatorni i etički okvir

Regulisanje veštačke inteligencije predstavlja jedan od najvećih institucionalnih izazova savremenih demokratija. Države širom sveta usvajaju regulatorne pristupe koji se kreću od potpunog oslanjanja

na samoregulaciju tržišta, kao što je to slučaj u Sjedinjenim Američkim Državama, gde vladajući okvir ostaje fragmentisan između sektorskih agencija (*FTC, FDA, NIST*) (Brundage et al., 2018), preko hibridnih modela koje promovišu *OECD* Principi o VI (2019), pa sve do sveobuhvatnih zakonskih okvira poput evropskog *AI Act-a*. Zajednički cilj ovih instrumenata jeste obezbeđivanje bezbednosti, pouzdanosti i transparentnosti algoritamskih sistema, uz istovremeno očuvanje inovativnog potencijala.

Evropski AI Act

Uredba Evropskog parlamenta i Saveta (EU) 2024/1689, poznata kao *AI Act*, predstavlja prvi sveobuhvatni pravni akt koji uređuje VI na tržištu, nadzor, sertifikaciju i korišćenje sistema veštačke inteligencije (European Parliament, 2024). Ova uredba uvodi pristup zasnovan na proceni rizika (*risk-based approach*), koji je konceptualno srodan sa pristupom koji se primenjuje u regulisanju medicinskih uređaja, farmaceutskih proizvoda i nuklearnih postrojenja (Veale, Borgesius, 2021).

AI Act razvrstava sve VI-sisteme u četiri kategorije, zavisno od stepena rizika koji nose:

- **Zabranjene prakse.** Ove prakse se odnose na sisteme koji dugoročno mogu naneti štetu korisnicima i građanima. Odnose se na uvođenje socijalnog kredita koji vrednuje građane na osnovu ponašanja, na biometrijsku kategorizaciju na osnovu osetljivih karakteristika i manipulativne tehnike koje eksploatišu psihološke ranjivosti (čl. 5 *AI Act*).
- **Sistemi visokog rizika.** Sistemi visokog rizika se odnose na one koji se primenjuju u zdravstvu, transportu, socijalnim uslugama, zapošljavanju, upravljanju kritičnom infrastrukturom i biometrijskoj identifikaciji (Aneks III *AI Act*).
- **Sistemi ograničenog rizika.** Kod ovih sistema se zahteva transparentnost, na primer četbotovi (*chatbots*) koji moraju eksplicitno otkriti da su *AI sistemi* (čl. 50 *AI Act*).
- **Minimalni rizik.** Obuhvata većinu aplikacija kao što su filteri za neželjenu poštu i sistemi koji nam preporučuju, gde se ne zahtevaju dodatne obaveze.

Za Republiku Srbiju su naročito relevantne odredbe koje se odnose na: obavezne sisteme upravljanja kvalitetom (čl. 17), obavezno ocenjivanje usaglašenosti pre stavljanja na tržište (čl. 43–44), vođenje tehničke dokumentacije (čl. 11), nadzor posle stavljanja na tržište (čl. 72) i zahteve za modele opšte namene – GPAI (čl. 51–56). Ove odredbe direktno oblikuju uslove pristupa jedinstvenom digitalnom tržištu EU. Primena ovih odredbi može imati ekonomske efekte za srpsku privredu.

GDPR i prava građana u kontekstu veštačke inteligencije

Kada govorimo o zaštiti građana, korisnika VI i podacima koji se daju prilikom otvaranja naloga, pristupa platformama i sistemima zasnovanim na VI, kao i podacima koje VI koristi za učenje, za sada Opšta uredba o zaštiti podataka (GDPR, Uredba EU 2016/679) ostaje ključni normativni okvir. Budući da se gotovo svaki savremeni VI sistem zasniva na masovnoj obradi podataka o ličnosti (Wachter, Mittelstadt & Floridi, 2017). *GDPR* uvodi set principa koji ograničavaju način na koji se podaci mogu koristiti za učenje, podešavanje i operativni rad algoritamskih modela.

U Republici Srbiji je *GDPR* transponovan kroz Zakon o zaštiti podataka o ličnosti (Službeni glasnik RS, br. 87/2018). Ovaj zakon uvodi minimalnu obradu podataka, zakonitu osnovu obrade, informisanje korisnika i prava ispitanika. Takođe, zakon uvodi i pristup, ispravku i brisanje podataka.

Posebno je značajan član 22 *GDPR* koji garantuje da lični podaci koji obradom proizvode pravne ili slične efekte ne budu predmet isključivo automatizovanog odlučivanja, već da u tom lancu odlučivanja postoji uloga čoveka. Ovo se odnosi na *VI-sisteme* koji se koriste u određivanju kreditnog rejtinga, selekciji kandidata ili upravljanju socijalnim davanjima.

Jedno pitanje se posebno ističe i odnosi se na profilisanje (čl. 4 *GDPR*), biometrijske obrade (čl. 9), medicinske podatke i analitiku visokog rizika, gde su obaveze rukovaoca ovakvim sistemima i podacima koje koriste u najvećoj meri restriktivne.

Uzajamni odnos i povezanost *GDPR*-a i *AI Act*-a formira dvostruki normativni štiti koji treba sagledati celovito u procesu razvoja i primene VI-sistema (Mantelero, 2018).

Standardizacija – ISO/IEC

Tehnički standardi iako na prvu misao nemaju direktne veze sa regulatornim okvirom, ipak su dobra osnova za sprovođenje regulatornih zahteva.

Standardi su korisni jer omogućavaju da na tržište mogu biti stavljeni samo sistemi VI koji su usklađeni sa relevantnim tehničkim specifikacijama.

Od standarda treba izdvojiti:

- **ISO/IEC 42001:2023 – Sistem upravljanja veštačkom inteligencijom**

Prvi globalni standard ove vrste, koji definiše zahteve za uspostavljanje, implementaciju, održavanje i kontinuirano unapređenje sistema upravljanja VI u organizacijama (ISO, 2023a).

- **ISO/IEC 23894:2023 – Upravljanje rizicima u oblasti VI**

Pružna smernice za identifikaciju, procenu i tretman rizika koji proističu iz primene VI-sistema, u skladu sa opštim okvirom ISO 31000 (ISO, 2023b).

- **ISO/IEC 38507:2022 – Upravljanje korišćenjem VI u organizacijama**

Delegira odgovornost organa upravljanja (korporativnih odbora) za stratešku primenu VI.

- **ISO/IEC 29100:2011 – Okvir privatnosti**

Odnosi se na VI-sisteme koji obrađuju podatke o ličnosti, komplementarno sa zahtevima GDPR-a.

Pored navedenih, *Evropski odbor za standardizaciju (CEN/CENELEC)* razvija harmonizovane standarde koji će biti podrška primeni *AI Act*-a, a koji će, u skladu sa *Sporazumom o stabilizaciji i pridruživanju*, biti primenjeni i u Srbiji.

Regulatorni okvir Republike Srbije

Razvoj normativnog okvira za veštačku inteligenciju u Srbiji odvija se na preseku domaće digitalne agende i procesa harmonizacije sa normama Evropske unije. Ovaj proces karakteriše postepen ali konsistentan napredak. Ishod ovog procesa i regulisanja upotrebe i razvoja

VI treba da bude po ugledu na *AI Act* ali da odražava i specifičnosti srpskog privrednog, društvenog i kulturnog konteksta.

Strateška osnova razvoja VI u Srbiji počiva na dva ključna dokumenta.

1. *Strategija razvoja veštačke inteligencije Republike Srbije* (Vlada RS, 2019) koja postavlja ciljeve u oblastima obrazovanja, nauke, privrede i javne uprave, uz naglasak na etičkim i bezbednosnim aspektima;
2. *Strategija razvoja industrije 4.0* (Vlada RS, 2020). Dokument koji se odnosi na primenu pametnih sistema u industriji, prepoznajući VI kao ključnu tehnologiju četvrte industrijske revolucije (Schwab, 2016).

S obzirom na to da Srbija teži harmonizaciji sa pravom EU u okviru procesa pristupanja, *AI Act* će u velikoj meri oblikovati domaće zakonodavstvo, posebno u delu tehničkih propisa, zaštite potrošača i regulisanja digitalnog tržišta (Fibriyanita, 2024).

Prema izveštajima Evropske komisije o napretku Srbije, oblast digitalne transformacije i vladavine prava algoritama prepoznata je kao jedno od prioriteta u procesu EU integracija, sa posebnim naglaskom na usklađivanje u oblasti zaštite podataka i elektronskih komunikacija.

U Srbiji je u toku izrada prvog *Zakona o veštačkoj inteligenciji*, koji predstavlja ključni normativni iskorak u uređivanju ove oblasti. Model koji je u pripremi, zasnovan je na konsultacijama sa institucijama, privredom i naučnom zajednicom.

Na osnovu gorenavedenih činjenica možemo navesti neke segmente koje bi zakon trebalo da reguliše:

- Pravila za stavljanje *AI* sistema na tržište, zasnovana na pristupu proceni rizika kompatibilnom sa *AI Act*-om.
- Institucionalni okvir za nadzor i praćenje primene, uključujući pitanje nadležnog regulatornog tela.
- Režim za modele opšte namene (malog rizika) koji prate globalne trendove regulisanja velikih jezičkih modela.
- Transparentnost algoritamskog odlučivanja prema fizičkim licima.
- Odgovornost proizvođača i korisnika VI-sistema, sa jasnom raspodelom obaveza u lancu vrednosti.

Ovaj zakon treba da bude deo šire legislative koja uključuje izmene Zakona o zaštiti podataka o ličnosti, Zakona o elektronskim komunikacijama i sektorskih propisa.

Diskusija

U ovom delu rada biće ukazano na pitanja i nedoumice u primeni veštačke inteligencije.

Regulatorna debata o veštačkoj inteligenciji odražava dublje ideološke, ekonomske i civilizacijske nedoumice savremenog društva. Analiza prikazana u ovom radu ukazuje na nekoliko ključnih nalaza.

- Prvo, na globalnom nivou jasno je definisano da se regulisanje VI zasniva na proceni i smanjenju rizika. Od svih postojećih normativnih akata *AI Act* Evropske unije zauzima centralnu poziciju kao akt koji garantuje najveću bezbednost i sveobuhvatno reguliše ovu oblast. Ovaj pristup svojim ograničenjima i smanjenjem rizika nije ograničio podsticanje inovacija za sisteme niskog rizika i striktnu kontrolu primena koje mogu ugroziti osnovna prava i bezbednost.
- Drugo, stanje je u Srbiji dinamično po pitanju razvoja, primene i regulisanja VI. Teži se ka usaglašavanju sa evropskim trendovima, ali se ne odustaje od ubrzanog napretka. Srbiji u ovom procesu može pomoći iskustvo zemlje poput Estonije koje pokazuje da manje države mogu postići visok nivo digitalne zrelosti upravo kroz usmerena javna ulaganja i jasne strategije (Drechsler, 2023).

Regulacija u SAD i EU

Ova dva regulatorna modela su u stvari dva različita pristupa koji imaju i različite posledice. Ovo je ne samo tehnička razlika u pristupu, već i odraz fundamentalno različitih vrednosnih sistema. EU je odabrala model zasnovan na prethodno definisanim pravilima koji postavljanjem jasnih granica pre plasiranja sistema na tržište nastoji da zaštiti prava građana i spreči štetne primene. SAD, naprotiv, istorijski preferira intervenisanje tek nakon što se šteta dogodi, oslanjajući se na tržišnu samoregulaciju i sektorsku kontrolu od strane agencija kao što su *FTC* i *FDA* (Calo, 2017).

Ova razlika ima direktan uticaj na privredu. Američki pristup, koji omogućava i stimuliše razvoj, a potom kontroliše, u osnovi je povoljniji za inovacije. Ovaj model smanjuje administrativne troškove usklađivanja i ubrzava plasman novih rešenja. Sa druge strane, kritičari ukazuju da ovaj pristup nosi ozbiljne sistemske rizike: primeri kazni prema kompanijama kao što su Meta, OpenAI i Amazon pokazuju da tržišna samoregulacija nije dovoljna tamo gde su u pitanju osnovna prava, psihološki integritet korisnika ili bezbednost kritične infrastrukture (Wachter, Mittelstadt & Floridi, 2017).

Posebno je indikativno da je nova američka administracija ukinula prethodnu Izvršnu naredbu o bezbednoj i pouzdanoj VI Izvršnu naredbu 14110 (*Executive Order 14110* iz oktobra 2023) i usmerila regulatornu agendu ka stimulisanju razvoja, eksplicitno distancirajući se od evropskog modela. Ovo je za evropske institucije i za države kandidate poput Srbije signal da harmonizacija sa EU standardima podrazumeva i preuzimanje određenih konkurentskih troškova u kratkom roku – uz potencijalnu dugoročnu dobit u vidu pravne sigurnosti i poverenja korisnika (Veale & Borgesius, 2021).

Za privredu, odgovor na pitanje koji model je bolji zavisi od konteksta. Za korisnike i građane, evropski model nudi veću zaštitu – posebno u oblastima profilisanja, automatizovanog odlučivanja i biometrijske identifikacije. Za kompanije koje razvijaju inovativna rešenja na novim tržištima, rigidnija regulacija može usporiti razvoj i favorizovati ekonomski moćnije aktere koji mogu da finansiraju skupu proceduru usklađivanja. Ova dilema nije razrešena ni u akademskoj literaturi ni u regulatornoj praksi (Doshi-Velez & Kortz, 2017).

Primena VI bez kontrole

Ovakav model, regulisanja ili neregulisanja može dovesti do zloupotrebe.

Primena VI-sistema bez adekvatnog nadzora dovodi do rizika. Izdvojicemo nekoliko rizika koji su navedeni u naučnoj literaturi.

- **Rizik od pristrasnosti algoritama.** Modeli obučeni na istorijskim podacima reprodukuju i pojačavaju društvene nejednakosti u oblastima zapošljavanja, kreditiranja i pravosuđa (O'Neil, 2016). Istraživanja su pokazala da komercijalni sistemi prepoznavanja

lica imaju znatno viši procenat grešaka za žene tamnijeg tena u poređenju sa belim muškarcima, što direktno utiče na ishode kada se takvi sistemi primenjuju u policijskom radu ili graničnoj kontroli (Buolamwini & Gebru, 2018).

- **Rizici po psihološki integritet korisnika.** Konkretna primer je tužba porodice američkog dečaka koji je izvršio samoubistvo, u kojoj se tvrdi da je dizajner Čet-Dži-Pi-Tija (*ChatGPT-a*) namerno stvarao psihološku zavisnost.¹ Ovaj primer ilustruje kako model zasnovan na maksimizaciji angažovanja korisnika može biti u direktnom sukobu sa zaštitom mentalnog zdravlja, naročito maloletnih korisnika. Istraživanja iz psihologije digitalnih medija potvrđuju da sistemi zasnovani na potkrepljujućim algoritmima mogu indukovati obrasce zavisnog ponašanja kod ranjivih grupa (Montag et al., 2021).
- **Rizik od zloupotrebe baza podataka i neovlašćeno profilisanje.** Kompanije ne razumeju koliki broj podataka o ličnosti je ušao u alate za veštačku inteligenciju i šta se radi sa njima. Ovo nije samo problem svesti, već i problem arhitekture. Veliki jezički modeli (*LLM*) koriste podatke o ličnosti tokom faze učenja i potencijalno ih reprodukuju u odgovorima, narušavajući pravo na privatnost čak i kada korisnici toga nisu svesni. Reidentifikacija anonimizovanih skupova podataka izvodljiva je u znatnom procentu slučajeva (Narayanan & Shmatikoff, 2008).
- **Rizici po kritičnu infrastrukturu.** Poznat je slučaj globalnog ispada interneta uzrokovanog greškom jednog inženjera u *AWS* sistemu, koji je ukazao na sistemsku ranjivost infrastrukture zavisne od algoritamskih sistema.²

Veštačka inteligencija u obrazovanju

Ovo je možda i najveći izazov za društvo i zakonodavce, izazov koji se ne sme ignorisati.

Jedna od najznačajnijih, a istovremeno najslabije regulisanih oblasti primene VI jeste obrazovanje. Generativni AI-sistemi u

¹ Vest je dostupna na <https://www.bbc.com/news/articles/cgerwp7rdlvo>

² <https://rs.bloombergadria.com/tehnologija/digitalizacija/91353/prekid-cloudflarea-blokirao-sajtove-chatgpt-ja-x-a-i-drugih/news>

svakodnevnoj su upotrebi kod učenika i studenata, transformišući ne samo načine učenja već i samu prirodu znanja, kreativnosti i akademskog integriteta (Holmes et al., 2022). Ovaj fenomen otvara niz pitanja na koja ni zakonodavstvo ni pedagoška nauka još uvek nemaju jasan odgovor.

Nastavni kadar nije opremljen da kritički sagledava ni da pedagoški prenosi znanja o VI, dok učenici samostalno i nekritički usvajaju njene koristi kao autoritativne izvore. Istraživanja potvrđuju da studenti koji koriste generativne AI alate bez kritičke refleksije razvijaju površinsko razumevanje nastavnog gradiva i smanjenu sposobnost argumentacije (Kasneci et al., 2023).

Istovremeno, VI nosi izuzetan obrazovni potencijal. Učenje može da bude personalizovano, sa adaptivnim kurikulumima, automatskom identifikacijom teškoća u učenju i podrškom inkluzivnom obrazovanju kroz asistivne tehnologije i izradu, primenu i evaluaciju IOP-a.

Pitanje nije da li VI treba da bude u učionici, već pod kojim uslovima, s kojim ciljevima i uz koje zaštitne mehanizme (Luckin et al., 2016). Odgovor na ovo pitanje mora biti interdisciplinaran, pravno regulisan i u okviru prava, pedagogije i etike.

U Srbiji, primenom *AI Act*-a i njegovom integracijom sa našim zakonodavstvom neće direktno biti regulisana primena VI u obrazovanju, osim u delu sistema visokog rizika (npr. platforme za ocenjivanje i praćenje učenika). Strategija razvoja VI Srbije prepoznaje obrazovanje kao prioritetnu oblast, ali konkretni akcioni planovi za kurikularne izmene i obuku nastavnika još uvek nedostaju. Potrebno je, najverovatnije obrazovni sistem reformisati od osnovne škole naviše, ne u smislu programiranja algoritama, već u smislu razumevanja konteksta, etičkih posledica i kritičke evaluacije AI sistema.

Pitanje uloga i odgovornosti

U primeni sistema koji koriste VI postoji nekoliko kategorija uloga koje treba razlikovati (rukovaoci, obrađivači i algoritamski lanci) i u odnosu na njih kreirati regulatoni okvir.

Ovo je ujedno i jedno od najtežih praktičnih pitanja u primeni regulatornih okvira – napraviti jasno razgraničenje odgovornosti između različitih aktera u lancu VI sistema. *AI Act* uvodi kategorije ponuđača, korisnika u poslovne svrhe, uvoznika i distributera, čije se definicije u kontekstu VI sistema ne poklapaju uvek sa klasičnim ulogama

rukovaoca i obrađivača iz *GDPR*-a. Ovo je naročito kompleksno u slučajevima kada kompanija angažuje spoljnog dobavljača za razvoj algoritamskog modela koji potom sama koristi u donošenju kadrovskih ili kreditnih odluka. Ovde se mešaju uloge, pa je dobavljač formalno i obrađivač, ali faktički ima znatan uticaj na ishode koji pogađaju fizička lica. Ova situacija nije adekvatno adresirana ni u *GDPR*-u ni u *AI Act*-u i predstavlja polje za buduće regulatorno preciziranje.

Sličan problem nastaje u oblasti ugovornih odnosa kada kompanije koriste medicinsku dokumentaciju ili onkološke snimke za razvoj dijagnostičkih modela. Pitanje ko je rukovalac nad medicinskim podacima korišćenim za obuku modela – zdravstvena ustanova, *IT kompanija* ili akademska institucija.

Ovo je posebno relevantno za Srbiju, gde zdravstveni sektor ulazi u fazu digitalizacije a regulatorna infrastruktura nije u potpunosti pripremljena za ove scenarije.

Takođe, o ovome se mora voditi računa kada se državni informacioni sistemi, podržani VI koriste za ostvarivanje prava socijalno ugroženih grupa (Maslikovic et al., 2026).

Brzina tehnologije nasuprot brzini regulacije

Najveća dilema u regulisanju VI je ona koja nastaje kada postoji namera da se održi razvojna priroda tehnologije i započne normativni proces. Tehnologija se razvija mnogo brže od regulative i to izaziva problem koji akademska literatura naziva *pejsing problem* (*paceing problem*) – strukturna nesposobnost regulatornih sistema da prihvate tempo tehnoloških promena (Marchetti, 2019).

Na tržištu se već nalaze generativni modeli koji se koriste u zapošljavanju, medicinskom odlučivanju i sudskim preporukama, dok zakoni koji bi regulisali ove primene još nisu ni u nacrtu. Posebno je zabrinjavajuće zapošljavanje, poslodavci sve češće primenjuju algoritamske sisteme za selekciju kandidata na osnovu analize CV-ja (*CV – curriculum vitae*), tona glasa ili mikroizraza lica, bez ikakve regulatorne kontrole i bez mogućnosti za kandidate da ospore takve odluke (Raghavan et al., 2020). Odredba o pravu na objašnjenje automatizovane odluke iz člana 22 *GDPR*-a teorijski pokriva ovu situaciju, ali je njena primena u praksi izuzetno slaba zbog nedostatka tužbi i institucionalnog kapaciteta nadzornih organa.

Moguća rešenja za problem neusklađenosti tempa (*paceing problem*) uključuju regulatorne prakse koje dozvoljavaju eksperimentisanje pod nadzorom, adaptivnu regulaciju koja predviđa mehanizme revizije propisa u kratkim ciklusima, kao i princip tehnološke neutralnosti koji zakon vezuje za rizike i ishode, a ne za konkretne tehnologije. Akt o veštačkoj inteligenciji delimično usvaja ove pristupe. Mada, iskustva iz Srbije nam govore da je značajno akumulirana neadekvatna komunikacija u državnim organima, odnosno da informacioni sistemi, digitalni alati i eUprava podržana VI nisu u potpunosti ispunili očekivanja i ulaganja (Masliković, Tomić, 2024).

Zaključak

Analiza međunarodnih okvira i uvida u literaturu ukazuje na to da ne postoji jedinstveni model regulacije veštačke inteligencije koji je istovremeno optimalan za privredu, građane i javni interes. Izgradnja regulatornog okvira zasnovanog na proceni rizika, usklađenog sa GDPR-om i sektorskim propisima, uz jačanje institucionalnih kapaciteta i podršku digitalnoj pismenosti, predstavlja neophodno rešenje.

Za Srbiju, proces harmonizacije sa normama Evropske unije ne bi trebalo da predstavlja samo formalno ispunjavanje zahteva, već stratešku odluku da se izgradi kvalitetan i održiv sistem regulisanja, kontrole i upravljanja sistemima veštačke inteligencije. Ovaj zadatak podrazumeva da se različiti akteri – ministarstva, naučne institucije, privreda i civilno društvo – aktivno uključe i zajednički rade na rešavanju ovog izazova. Zakon o veštačkoj inteligenciji neće biti dovoljan sam po sebi; on mora biti deo šire legislative, praćen odgovarajućim podzakonskim aktima, smernicama za primenu i mehanizmima za redovnu reviziju.

LITERATURA

- Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ... Amodei, D. (2018). *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation*. Oxford: Future of Humanity Institute, University of Oxford. <https://doi.org/10.48550/arXiv.1802.07228>
- Buolamwini, J. & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. In: S. A. Friedler & C. Wilson (Eds.), *Proceedings of the 1st Conference on Fairness, Accountability*

- and Transparency (PMLR Vol. 81, pp. 77–91). <https://proceedings.mlr.press/v81/buolamwini18a.html>
- Calo, R. (2017). Artificial intelligence policy: A primer and roadmap. *UC Davis Law Review*, 51(2), 399–435. https://lawreview.law.ucdavis.edu/sites/g/files/dgvnsk15026/files/media/documents/51-2_Calo.pdf
- Doshi-Velez, F., Kortz, M., Budish, R., Bavitz, C., Gershman, S., O'Brien, D., ... Wood, A. (2017). *Accountability of AI under the law: The role of explanation*. Cambridge, MA: Berkman Klein Center Working Group on Explanation and the Law. <https://doi.org/10.2139/ssrn.3064761>
- Drechsler, W. (2023). Estonian e-governance and artificial intelligence: A case study in digital transformation. *Government Information Quarterly*, 40(2), 101–115. <https://doi.org/10.1016/j.giq.2022.101789>
- European Parliament, Council of the European Union (2016). *Uredba (EU) 2016/679 o zaštiti pojedinaca u vezi sa obradom ličnih podataka i o slobodnom kretanju takvih podataka (Opšta uredba o zaštiti podataka)*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679>
- European Parliament, Council of the European Union (2024). *Uredba (EU) 2024/1689 o utvrđivanju usklađenih pravila o veštačkoj inteligenciji (Akt o veštačkoj inteligenciji)*. <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32024R1689>
- Fibriyanita, F. (2024). The rise of artificial intelligence (AI) in public administration: Reimagining government services and delivering value to citizens. *Public Studies and Business Administration Journal (PUSBA)*, 1(1), 72–80.
- Holmes, W., Bialik, M. & Fadel, C. (2019). *Artificial intelligence in education: Promises and implications for teaching and learning*. Boston: Center for Curriculum Redesign.
- International Organization for Standardization [ISO] (2023a). *ISO/IEC 42001:2023 Information technology—Artificial intelligence—Management system*. Geneva: ISO.
- ISO (2023b). *ISO/IEC 23894:2023 Information technology—Artificial intelligence—Guidance on risk management*. Geneva: ISO.
- Kasneci, E., Sessler, K., Küchemann, S., Bannert, M., Dementieva, D., Fischer, F., ... Kasneci, G. (2023). ChatGPT for good? On opportunities and challenges of large language models for education. *Learning and Individual Differences*, 103, Article 102274. <https://doi.org/10.1016/j.lindif.2023.102274>
- Luckin, R., Holmes, W., Griffiths, M. & Forcier, L. B. (2016). *Intelligence unleashed: An argument for AI in education*. London: Pearson.
- Mantelero, A. (2018). AI and big data: A blueprint for a human rights, social and ethical impact assessment. *Computer Law & Security Review*, 34(4), 754–772. <https://doi.org/10.1016/j.clsr.2018.05.017>
- Marchetti, I. (2019). Hopelessness: A network analysis. *Cognitive Therapy and Research*, 43, 611–619. <https://doi.org/10.1007/s10608-018-9981-y>

- Maslikovic, D., Tomic, B., Kadijevic, Dj. (2026). Factors influencing accessibility in judicial institutions for people with disabilities: a study of the Serbian judicial system. *Humanities and Social Sciences Communications, Nature*. <https://doi.org/10.1057/s41599-026-06762-7>
- Masliković, D., Tomić, B. M. (2024). Is there communication? Access to information by persons with disabilities in Serbi, *Stanovništvo*, 62(1), 153–166. <https://doi.org/10.59954/stnv.563>
- Montag, C., Lachmann, B., Herrlich, M. & Zweig, K. A. (2019). Addictive features of social media/messenger platforms and freemium games against the background of psychological and economic theories. *International Journal of Environmental Research and Public Health*, 16(14), Article 2612. <https://doi.org/10.3390/ijerph16142612>
- Narayanan, A. & Shmatikov, V. (2008). Robust de-anonymization of large sparse datasets. In: *2008 IEEE Symposium on Security and Privacy* (pp. 111–125). Piscataway, NJ: IEEE. <https://doi.org/10.1109/SP.2008.33>
- Organisation for Economic Co-operation and Development [OECD] (2019). *Recommendation of the Council on artificial intelligence (OECD/LEGAL/0449)*. Paris: OECD. <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>
- O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. New York: Crown.
- Raghavan, M., Barocas, S., Kleinberg, J. & Levy, K. (2020). Mitigating bias in algorithmic hiring: Evaluating claims and practices. In: *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (pp. 469–481). New York: Association for Computing Machinery. <https://doi.org/10.1145/3351095.3372828>
- Russell, S. & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson.
- Schwab, K. (2016). *The fourth industrial revolution*. Geneva: World Economic Forum.
- Veale, M. & Zuiderveen Borgesius, F. J. (2021). Demystifying the draft EU Artificial Intelligence Act. *Computer Law Review International*, 22(4), 97–112. <https://doi.org/10.9785/cr-2021-220402>
- Strategija razvoja veštačke inteligencije u Republici Srbiji za period 2020–2025, *Službeni glasnik RS*, br. 96/2019.
- Wachter, S., Mittelstadt, B. & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, 7(2), 76–99. <https://doi.org/10.1093/idpl/ix005>
- Zakon o zaštiti podataka o ličnosti, *Službeni glasnik RS*, br. 87/2018.

Artificial Intelligence between Innovation and Regulation: International and National Regulatory Framework with Special Reference to the Republic of Serbia

Abstract

The accelerated development of artificial intelligence (AI) systems has once again raised the question of balancing innovation with the protection of public interests. This paper analyzes current international regulatory frameworks – primarily the European Union’s Artificial Intelligence Act (AI Act, 2024), the General Data Protection Regulation (GDPR), and key standards from the ISO/IEC series – and examines their implications for regulatory development in the Republic of Serbia. Particular attention is given to the process of drafting the first AI law in Serbia, strategic documents guiding the development of the digital economy, and obligations arising from the country’s accession process to the European Union. The paper argues that a comprehensive, risk-based approach to AI regulation does not necessarily hinder innovation; rather, it can serve as a foundation for building user trust, ensuring legal certainty for businesses, and achieving long-term technological sovereignty.

Keywords: artificial intelligence, regulation, AI Act, GDPR, ISO/IEC 42001, Serbia, digital transformation, risk management